REMARKS

Claims 1-20 are currently pending in the present application and are presently under consideration. All pending claims with status identifiers are found at pages 2-4.

Favorable reconsideration is requested in view of the comments below.

I. **Rejection of Claims 1-5, 7-8, 10, 12-14, and 17-19 Under U.S.C. §102(e)**

Claims 1-5, 7-8, 10, 12-14 and 17-19 stand rejected under 35 U.S.C. §102(e) as being anticipated by McNabb, *et al.* (U.S. 6,289,462). Reconsideration and allowance of claims 1-5, 7-8, 10, 12-14, and 17-19 is respectfully requested for at least the following reasons. McNabb, *et al.*, does not disclose, teach, or suggest each and every element as recited in the subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

With respect to independent claims 1, 10, and 12, McNabb, *et al.* nowhere discloses a system and/or methodology for regulating access to a ***distributed computing platform***, let alone a ***module that requests access to the distributed computing platform*** as claimed. Further, McNabb, *et al.* does not disclose, teach, or suggest ***applying a trust level to the... module to regulate access to the distributed computing platform*** as recited in these claims. A distributed computing platform enables a large task to be segregated and completed by a plurality of disparate computers. Thus, applications can seek access to a plurality of computers within a distributed computing environment. Because ***distributed computing platforms*** require their infrastructure to be accessible so as to facilitate optimal distributed computing, security relating to such platforms is of extreme importance. The present invention provides this security ***via analyzing a first module and an application environment associated with the first module*** and ***determining a level of access to the distributed computing platform and applying a trust level to the***

first module corresponding to the determined level of access. Thus, for example, a module that desires access to a restricted area within the ***distributed computing platform*** is first analyzed prior to allowing access to such restricted area. If upon analysis the application is determined to be fully trusted, the application can have read/write privileges to the restricted area. If, however, the application is only partially trusted, the application can be granted read-only access. Further, if the application is not trusted at all, then the application can be completely denied access to the ***distributed computing platform***. Such application of a ***trust level*** as recited in the claim and defined within the specification is a benefit over conventional binary analysis systems.

In contrast to the present invention as claimed, McNabb, *et al.* nowhere discloses, teaches, or suggests a security system for ***a distributed computing platform***, much less ***applying a trust level via determining a level of access to a distributed computing platform*** as recited in these claims. Rather, McNabb, *et al.* teaches a *binary* security system for a *trusted server* (rather than a ***distributed computing platform*** as claimed), where a process or program is either allowed access to a portion of the trusted server or denied access to a portion of the trusted server. *See* col. 9, lines 16-19; col. 12, lines 42-45; col. 13, lines 37-42. The disclosed benefit of the security system taught in McNabb, *et al.* is that individual programs/processes rather than individual users are assigned security labels, thus preventing a malicious user who managed to log into the server as an administrator from compromising an entire system. *See* col. 4, lines 34-37. The security system disclosed in McNabb, *et al.*, however, is not related to ***distributed computing platforms*** as recited in the aforementioned independent claims, as ***distributed computing platforms*** must leave itself accessible and/or modifiable by several users to be effective.

The portion of McNabb, *et al.* (col. 4, lines 34-57) does not disclose, teach, or suggest a security system for utilization in a ***distributed computing platform*** as claimed. Rather, col. 4, lines 34-57 teaches a server security system that utilizes pre-attached security labels to process(es) to maintain security within a server. Particularly, process(es) are assigned authorization levels that are verified at each process step, and the process(es) do not pass or inherit rights to other process(es). *See* col. 4, lines 45-50. Further, McNabb, *et al.* discloses separate users requesting the same item may obtain different results. *See* col. 4, lines 50-54. This is because different users may be assigned

different privileges, and may therefore have disparate access rights to the requested item. As before, this does not relate to a ***distributed computing platform*** as claimed.

In view of the foregoing, it is readily apparent that McNabb, *et al.* does not anticipate nor make obvious the subject invention as recited in claims 1, 10, and 12 (and claims 2-5, 7-8, 12-14, and 17-19 which respectfully depend there from). Accordingly, this rejection should be withdrawn.

II. Rejection of Claims 6, 9, 11, 15-16, and 20 Under 35 U.S.C. §103(a)

Claims 6, 9, 11, 15-16, and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over McNabb, *et al.* in view of McManis (U.S. 6,546,487). Reconsideration and allowance of claims 6, 9, 11, 15-16, and 20 is respectfully requested for at least the following reasons. McManis does not make up for the aforementioned deficiencies of McNabb, *et al.* with respect to independent claims 1, 10, and 12. Particularly, like McNabb, *et al.*, McManis does not disclose, teach, or suggest a security system utilized with respect to a ***distributed computing platform,*** much less ***applying the trust level to the first module to regulate access to the distributed computing platform*** as claimed. Therefore, this rejection should be withdrawn.

III. Conclusion

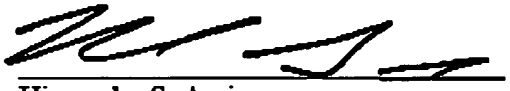
The present application is believed to be condition for allowance in view of the above comments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063.

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicant's undersigned representative at the telephone number listed below.

Respectfully submitted,

AMIN & TUROCY, LLP



Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731